SCIS 2022 2022 Symposium on
Cryptography and Information Security
Osaka, Japan & Online, Jan. 18 – 21, 2022
The Institute of Electronics,
Information and Communication Engineers

オンラインサンドボックスにおけるMITRE ATT&CKマッピング機能に係る実態調査

Survey on Mapping Function for Malware Behaviors to MITRE ATT&CK of Online Malware Sandbox

藤井 翔太 *† 山岸 伶 * 山内 利宏 ††
Shota Fujii Rei Yamagishi Toshihiro Yamauchi

キーワード MITRE ATT&CK, オンラインサンドボックス

あらまし

サイバー攻撃において，マルウェアは重要な役割を有しており，日々新たなマルウェアが大量に発見されている [1]．このような大量のマルウェアに対応するために，マルウェアを自動で解析する動的解析がデファクトとなっている．ここで，解析支援の一つとして，マルウェアの挙動をMITRE ATT&CK techniques [2] の各要素（以降，technique）にマッピングする機能が存在し，多くのオンラインサンドボックスにおいて採用されている．MITRE ATT&CK techniquesは，攻撃に利用される技術や戦法を整理したものである．マルウェアの挙動をこれらに自動でマッピングすることにより，効率的にマルウェアの機能概要を把握し，セキュリティオペレーションに活用することができる．

一方で，technique へのマッピングには、実装に依存する部分がある. 例えば, technique の一つである T1071（Application Layer Protocol）は，検知手法として Analyze network data for uncommon data flows (e.g., a client sending significantly more data than it receives from a server).と記載があるが，uncommon の一意的な定義が難しく，どのような通信を検出するかは実装に依存する．こうした部分に依って分析結果が左右される可能性があるため，各種オンラインサンドボックスにおける technique へのマッピング機能について，その実態を把握することがセキュリティオペレーションを遂行する上で重要である．

そこで，technique へのマッピング機能を有するオンラインサンドボックスを対象に，その実態を調査する．具体的には複数のオンラインサンドボックスの解析結果から technique へのマッピング結果を抽出し，それぞれ古い版の technique の最新版への名寄せ等の処理を行ったうえで以下の観点での調査を実施する（図 1）．

- オンラインサンドボックス間で technique マッピング機能に差異があるか．
- 機械的に抽出が可能な technique と困難な technique が存在するか．
- 偽陽性を生じやすい technique が存在するか．

本調査を通して，technique へのマッピング機能の実態を明らかにするとともに，活用に際してのベストプラクティスの導出を図る．

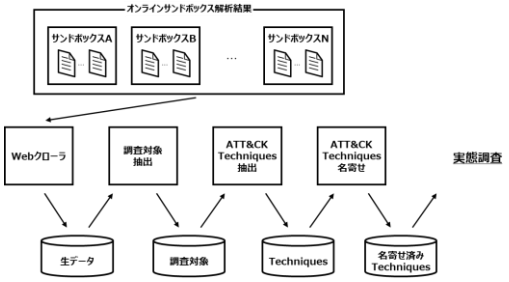

図 1 実態調査に係る全体像

参考文献

[1] AV-TEST: Malware Statistics & Trends Report, available from <https://www.av-test.org/en/statistics/malware/>
[2] MITRE: ATT&CK, available from <https://attack.mitre.org/>

* 株式日立製作所, 神奈川県横浜市戸塚区吉田町 292 番地, Hitachi, Ltd., 292, Yoshidacho, Totsuka-ku, Yokohama-shi, Kanagawa
† 岡山大学 大学院自然科学研究科, 岡山県岡山市北区津島中 3 丁目 1-1, Graduate School of Natural Science and Technology, Okayama University, 3-1-1 Tsushima-naka, Kita-ku, Okayama
†† 岡山大学 学術研究院自然科学学域, 岡山県岡山市北区津島中 3 丁目 1-1, Graduate School of Natural Science and Technology, Okayama University, 3-1-1 Tsushima-naka, Kita-ku, Okayama